Lab 06 - Graylog Hunting

# Question 1 - What network has the most association frames?

Graphical user interface, application

Description automatically generated

DSU\_Mobile with 30 frames

# Question 2 - Which sensor has collected the most frames total?

Graphical user interface, text, application

Description automatically generated

SC112 has the most frames.

# Question 3 - Which network has the most probe requests? Why are most probes wildcards (or null)?

A picture containing table

Description automatically generatedFirst, NULL

Second, GoTrojans.

Probe requests with a NULL or wildcard SSID, occur because there is no entry in the SSID field in the incoming probe request.

A client station is looking for any network to join by sending a probe request with the SSID set to null.

In doing so, all APs that hear the request should reply by sending a probe response.

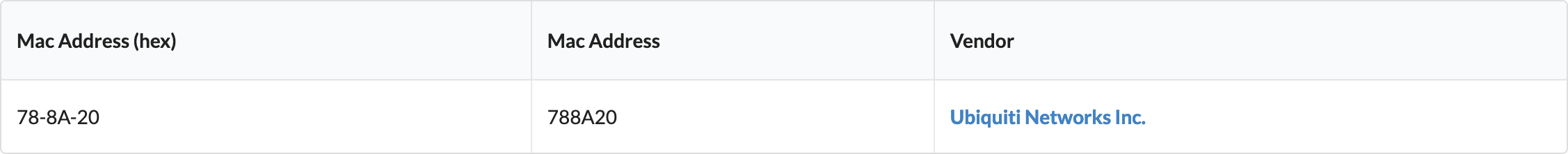
This is just one way that a client station can passively query new or known networks to connect.

# Question 4 - Who is the manufacturer of the network DSUnix?

Graphical user interface, text, application

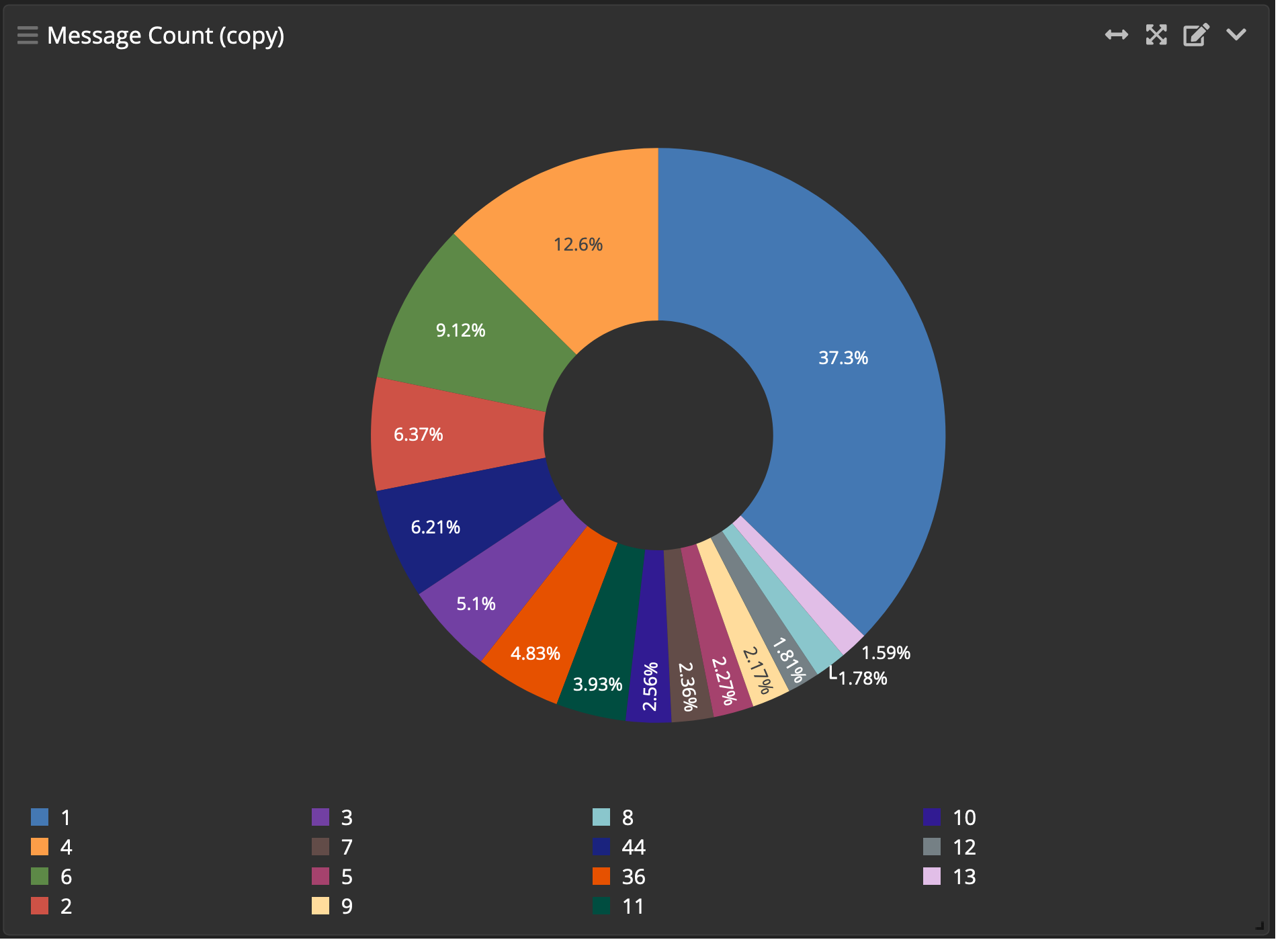
Description automatically generated

Looking up the sender address with the OUI reference tool shows us…



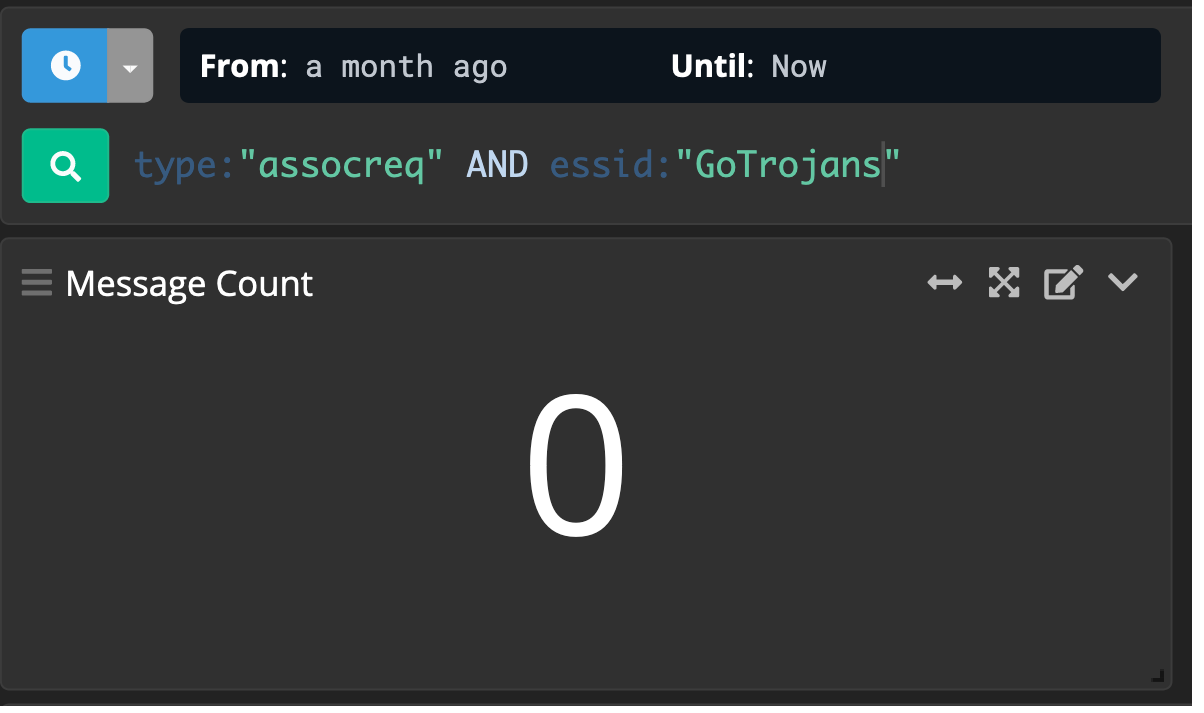
The AP belongs to Ubiquiti Networks Inc.

# Question 5 - What is the most popular channel in use?



Channel 1 has the most usage at 37.3% of all captured frames; 70,161 frames.

# Question 6 - How many association requests exist for GoTrojans?



Looking for the association requests specifically shows nothing.

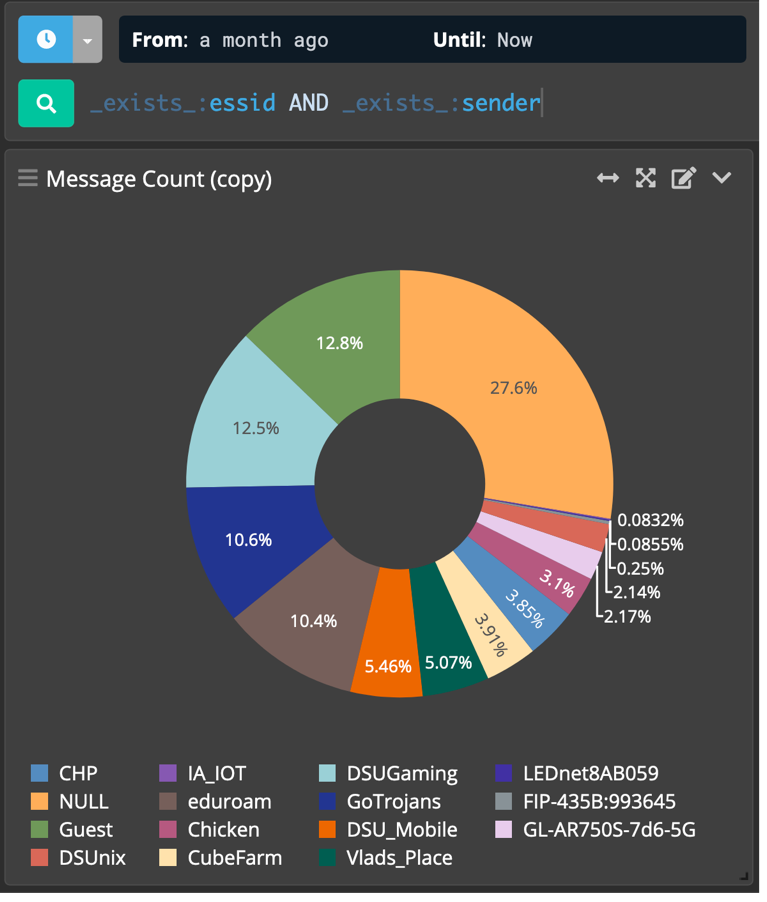
Graphical user interface

Description automatically generated

And here we just wanna verify that we can see traffic for GoTrojans – which we can.

Which means, nothing for GoTrojans. Nada. Zero association requests.

# Question 7 - Identify the SSID with the most BSSIDs



First, NULL (again)

Second, Guest

# Question 8 - A deauthentication attack occurred. What client was attacked specifically?

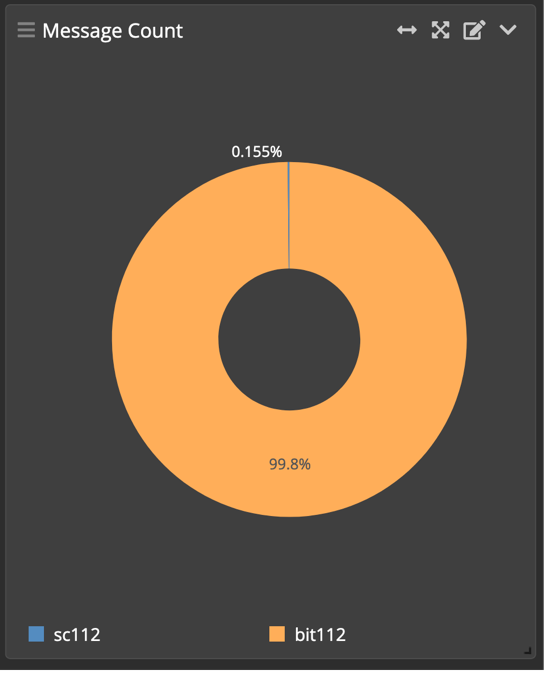
A screenshot of a computer

Description automatically generated with medium confidenceFirst, ec:08: 6b:bf:13:c4

Second, 00:c0:ca:a7:7f:73

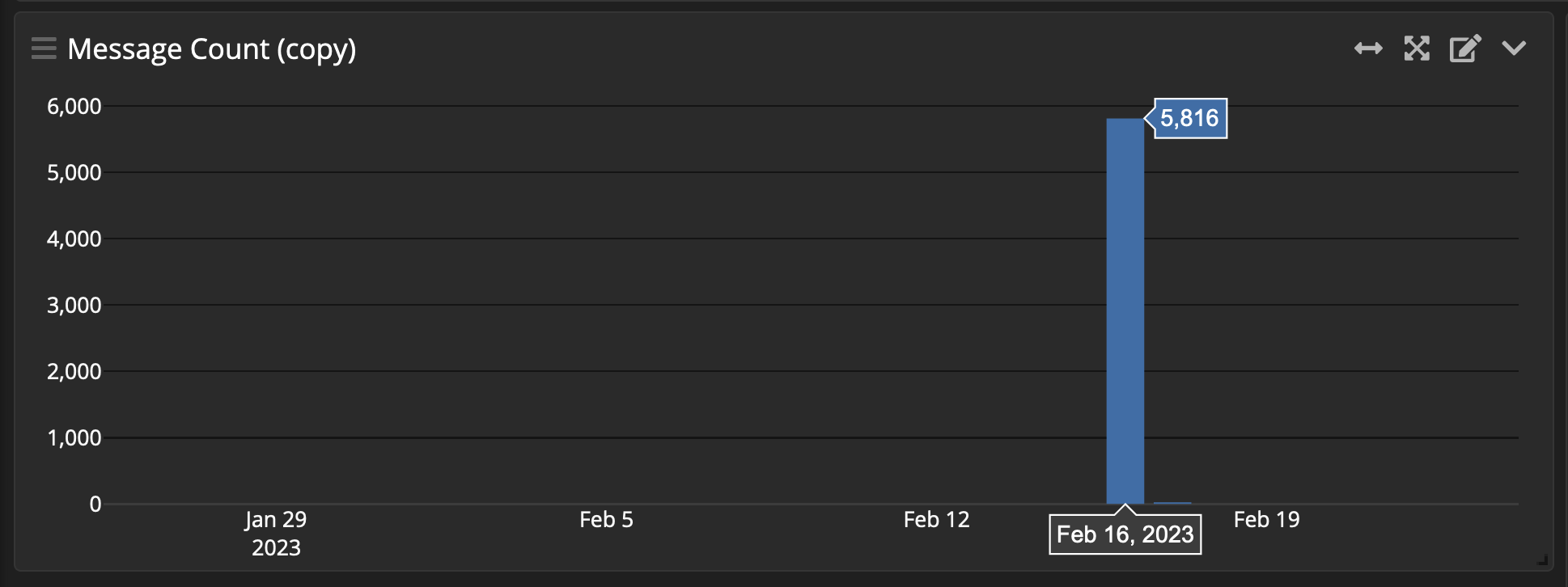
Difference of 0.4%

# Question 9 - Around where did the deauthentication attack take place (hint: think of the sensor names here, as they’re room numbers).

Primarily, BIT112…

So, the Beacom Institute of Tech building – Room 112

# Question 10 - What time did the deauthentication attack take place?



Feb 16th, 2023 – Specifically…

2023-02-16, 18:19 PM… until… 2023-02-17, 16:56 PM

# Question 11 - Identify the SSID or network that the client was DoS’d from in the deauthentication attack.

Graphical user interface

Description automatically generated

Looking up any frames where the recipients were targeted in the deauth attack and the ESSID exists, we can see that the primary network was DSU\_Mobile.

Interestingly, the address ec:08:6b:bf:13:c4 belongs to an AP for that network.

The adapter with the address 00:c0:ca:a7:7f:73, is likely the attacker… since Alfa adapters are preferred for WiFi attacks.

Graphical user interface, application, Teams

Description automatically generated

And the adapter with the address ec:08:6b:bf:13:c4, is likely the actual AP used by the network.

Table

Description automatically generated with medium confidence